REMARKS

Claims 1-60 are pending.

Claims 2-7, 20, 22-27, 40, 42-47 and 60 have been withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a non-elected species, there being no allowable or generic linking claim. Election was made without traverse in the reply files on June 27, 2005.

Claims 1, 12, 15, 19 and 20 have amended.

No new matter has been added as a result of the amendments presented herein.

CLAIM REJECTIONS

35 U.S.C. 102(e)

Claims 1, 8, 9, 19, 21, 28, 29, 39, 41, 48, 49 and 59 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Number 6,070,243 to See et al. (See). The rejection is respectfully traversed for the reasons below.

Claims 8, 9, and 19 depend from Claim 1; Claims 28, 29 and 39 depend from Claim 21; and Claims 48, 49, and 59 depend from Claim 41; each of which further define embodiments of the present invention. Claims 21 and 41 comprise similar limitations as those in Claim 1.

Claim 1 recites:

> In a network comprising a first electronic device and a second electronic device, a method for authenticating access to a controlled network, said method comprising:
> a) authenticating said second electronic device to said first electronic device, said first electronic device communicatively coupled to said second electronic device, said second electronic device an authentication server;

b) authenticating said first electronic device to said second electronic device, said first electronic device a client device;
c) determining a key at said first electronic device and at said second electronic device; and
d) authenticating a user to a central authentication server.

Thus, Applicants invention is directed to a method for authenticating access to a controlled network in which a central authentication server is authenticated to a client device and a client device is authenticated to a central authentication server in which an authentication key is determined by the client device and the central authentication server and that key is used in conjunction with the authentication method, as claimed.

See, as understood by Applicants, does not disclose authenticating a central authentication server to a client device nor does See disclose determining an authentication key at a client device or at the central authentication server, as claimed.

As understood by Applicants, See discloses a NMS (network management station) 20 that includes a server 320 that is configured with an authentication key associated with each authentication agent active on an edge device (10, 15) (Col. 5, lines 14-18) within a network 1 (Fig. 1, col. 1, lines 17-42; Fig. 3a, col. 5, lines 3-17).

As further understood by Applicants, See also suggests an edge device (10, 15) and the NMS (20) perform authentication using authentication keys configured on agent 400 (edge device 10, 15, Fig. 1; Fig. 2, col. 4, lines 43-54) and agent 320 of NMS 20 (Col. 5, lines 45-48).

See, as understood by Applicants, suggests an edge device (10, 15) each of which include an authentication agent 400 that is configured to, upon initialization of the edge device, establish a secure connection to a server 320 in NMS 20, in which agent 400 uses the known address of a server 320 to request a connection to server 320. See further suggests

that agent 400 and server 320 of NMS 20 utilize authentication keys stored on both edge device 10 and NMS 20 for authentication such that the NMS and the edge device mutually authenticate each other (Col. 5, lines 42-47).

To the extent that See discloses device authentication, Applicants understand See to suggest that an intelligent edge device 10 utilizing an agent 400 to authenticate a server 320, e.g., NMS 20, and NMS 20 authenticates an edge device 10. Subsequent thereto, See suggests that an edge device (10, 15) uses end system authentication performed by authentication agent 320, residing on NMS 20, to allow further communication (col. 5, lines 29 to col. 6, lines 45).

However, as understood by Applicants, See does not suggest, teach or describe "authenticating said second electronic device to said first electronic device, said first electronic device communicatively coupled to said second electronic device, said second electronic device an authentication server," as recited in Claim 1.

Continuing, as understood by Applicants, See discloses edge device 10 and server 320 provide authentication of each other through the utilization of pre-existing authentication keys.

Further, Applicants respectfully assert that See discloses the utilization of pre-existing authentication keys stored in the edge device and the NMS and which is/are used for the authentication of the edge device and the NMS. (Emphasis added)

With respect to determining an authentication key, See, as understood by Applicants, is silent as to any authentication key being determined by and generated from a client device

(end system), a network access point (edge device) or an central authentication server (NMS). Rather, See discloses utilization of existing authentication keys.

However, See does not suggest, teach or describe "determining a key at said first electronic device and at said second electronic device," as recited in Claim 1.

Continuing, Applicants respectfully assert that See suggests a first electronic device that is an intelligent edge device (Fig. 1, #10, #15; col. 4, lines 17-25) that may be associated with end systems 40, 50, and 60. However, See does not describe an edge device (Fig. 1, #10, #15) as an end system (client device). Thus, Applicants respectfully assert that See does not suggest, teach or describe "said first electronic device a client device," as required in Claim 1.

Because Applicants believe Claim 1 overcome the rejection under 35 U.S.C. 102(e) and as Claims 8, 9, and 19 depend from Claim 1 and Claims 28, 29 and 39 depend from Claim 21 and Claims 48, 49, and 59 depend from Claim 41, in which Claims 21 and Claim 41 comprise similar limitations as those in Claim 1, Applicants respectfully assert that the present invention, as claimed is not anticipated by See.

As such, Applicants respectfully assert that Claims 1, 8, 9, 19, 21, 28, 29, 39, 41, 48, 49 and 59 overcome the rejections of record and are in condition for allowance. Accordingly, Applicants respectfully request the rejection of Claims 1, 8, 9, 19, 21, 28, 29, 39, 41, 48, 49 and 59 under 35 U.S.C. 102(e) be withdrawn and Claims 1, 8, 9, 19, 21, 28, 29, 39, 41, 48, 49 and 59 be allowed.

35 U.S.C. 103(a)

Claims 10, 11, 30, 31,50 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over See as applied to Claims 9, 29, and 49, above in view of Applied Cryptography, Second Edition by Schneier, in further view of Computer Dictionary, Third Edition by Microsoft. Applicants respectfully traverse.

With regard to the Office Action's cited reference, Applicants understand Schneier to teach a Mutual Authentication Using The Interlock Protocol (Page 54).

Applicants respectfully point out that the third sentence in the introductory paragraph related to Mutual Authentication Using The Interlock Protocol specifically states "Here's a protocol that will not work." As such, Applicants respectfully assert that combining the teachings of Schneier with the teachings of See is contraindicated. Further, as the Mutual Authentication as disclosed by Schneier does not work; additional teachings combined therewith are also rendered inoperable.

As such, Applicants respectfully traverse the Office Action's assertion the one would be motivated to combine the teachings of Schneier with the teachings of See.

Accordingly, Applicants respectfully assert that Claims 10, 11, 30, 31, 50 and 51 are patentable over See in view of Schneier in further view of Microsoft. As such, Applicants respectfully request the rejections of Claims 10, 11, 30 31 and 51 under 35 U.S.C. 103(a) be withdrawn and Claims 10, 11, 30 31 and 51 be allowed.

35 U.S.C. 103(a)

Claims 10-17, 30-37, and 50-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over See, as applied to Claims 9, 29, and 49 above, in view of "PPP EAP TLS Authentication Protocol" by Adoba et al. (Adoba). Applicants respectfully traverse for the following reasons.

Applicants respectfully assert that the present invention addresses shortcomings within the EAP-TLS mutual authentication in that the EAP-TLS requires the deployment of a public key infrastructure (to support client-side certificates) and the key shared between the client device and the access point is also known (technically, the information used to generate it is known) by the authentication server (Instant Specification: Background; page 6, paragraph 2-3).

As such, combining the teaching of Adoba with the teaching of See does not remedy the shortcomings of See. As such, Applicants respectfully assert that Claims 10-17, 30-37, and 50-57 are rejected under 35 U.S.C. 103(a) are patentable over See, as applied to Claims 9, 29, and 49 above, in further view of Adoba.

Accordingly, Applicants respectfully request that the rejections of Claims 10-17, 30-37, and 50-57 under 35 U.S.C. 103(a) be withdrawn and that Claims 10-17, 30-37, and 50-57 be allowed.

35 U.S.C. 103(a)

Claims 18, 38, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over See, as applied to Claims 1, 21, and 41 above, in view of How Networks Work by Derfler, et al. (Derfler). Applicants respectfully traverse.

See, as understood by Applicants, specifically describes a wired network, such as an Ethernet or Token Ring network, in which an end station on an Ethernet network is able to communicate with an end station on a Token Ring network (Col. 4, lines 58 to col. 6, line 3) in which See discloses a plurality of switches (Omniswitch® and Pizzaswitch®) that are designed and configured for wire line communication.

Applicants respectfully assert that substantial modifications to the network of See would be necessary to combine the teachings of Derfler with the teaching of See. Further, with reference to See, combining Derfler therewith may not provide operability given the particular components and configuration as disclosed by See.

Because Applicants believe Claims 1, 21 and 41 to be allowable, Claims 18, 38 and 58 are also believed to be allowable. As such, Applicants respectfully request the rejections of claims 18, 38 and 58 under 35 U.S.C. 103(a) be withdrawn and Claims 18, 38 and 58 be allowed.

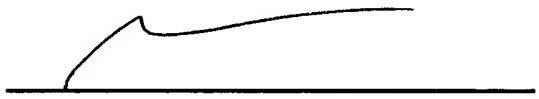
CONCLUSION

In light of the above listed amendments and remarks, reconsideration of the rejected Claims is requested. Based on the amendments and arguments presented above, it is respectfully submitted that Claims 1, 8-19, 21, 28-39, 41, and 48-59 overcome the rejections of record. Therefore, allowance of Claims 1, 8-19, 21, 28-39, 41, and 48-59 is earnestly solicited.

Should the Examiner have a question regarding the instant response, the Applicants invites the Examiner to contact the Applicants' undersigned representative at the below listed telephone number.

Respectfully submitted,
WAGNER, MURABITO & HAO LLP

Dated: 1/19, 2006



John P. Wagner
Registration No. 35,398

Address: WAGNER, MURABITO & HAO LLP
Watsonville Office:
Westridge Business Office
123 Westridge Drive
Watsonville, California 950765113

Telephone: (408) 938-9060 Voice
(408) 938-9069 Facsimile